UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

7590 12/21/2004

BRACEWELL & PATTERSON, L.L.P.
Intellectual Property Law
P.O. Box 969
Austin, TX 78767-0969

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/651,548	ATKINS ET AL.	
	Examiner	Art Unit	
	Kyung H Shin	2143	

-- The MAILING DATE of this c mmunication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is responding to application filed 8/29/2000

2. Claims **1 - 24** are pending. **Claims 1, 3, 6, 7, 9, 11, 14, 15, 17, 19, 23 are amended.** Independent claims are **1, 9, 17**.

Response to Arguments

3. Applicant's arguments, filed 5/18/2004, with respect to the rejection(s)of claim(s) 1-24 under Challener have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made under 35 U.S.C. 103(a).

Claim Rejection – 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 - 3, 6 - 11, 14 - 19, 22 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan et al. (US Patent No. 6,807,277) in view of Sudia (US Patent No. 6,009,177).

Regarding Claims 1, 9, 17 (currently amended), Doonan discloses a network messaging system. (see Doonan col. 1, lines 10-12: " *... present invention is directed to a secure electronic messaging system ...* ") Doonan discloses a method, a system and program product for managing a user key used to sign a message for a data processing system, said method comprising:

a) assigning a user key to a user and storing the user key in an encrypted data processing system utilized to encrypt messages; (see Doonan col. 2, lines 1-7: encryption key assigned by key server for message encryption)

b) encrypting the messages with the user key; (see Doonan col. 2, lines 7-8: message is encrypted)

c) storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key; (see Doonan col. 5, lines 63-67: generate an encrypted user key for transmission)

d) said encrypting data processing system communicating at least one encrypted messages together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; (see Doonan col. 6, line 1: encrypted message and encrypted key are transmitted to recipient)

f) computer usable media bearing said control program. (see Doonan col. 3, lines 9-12; col. 9, lines 33-44: software exists on computer readable medium for program execution)

e) Doonan discloses a check on the validation of a sender's credentials. (see Doonan col. 5, lines 16-20: sender credentials are verified) Doonan does not specifically disclose using a certificate authority (trusted third party) for key validation and determination of key revocation. However, Sudia discloses preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system (see Sudia col. 22, lines 51-63; col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to invalidate the association key when the status of the association key has been revoked as taught by Sudia. One of ordinary skill in the art would be motivated to employ Sudia in order to enable a trusted third party for a flexible and independent network key management system. (see Sudia col. 10, lines 23-25: *" ... provide a commercial key escrow system that uses private keys that may be changed by the user at will or at regular intervals ... "*; col. 11, lines 15-23: *" ... a system of certificate management ... very flexible and independent of location and time ... escrowing a private decryption key and receiving an escrow certificate ... registering a trusted device with a trusted third party and receiving authorization from that party enabling the device to communicate with other trusted devices ... "*)

Regarding Claims 2, 10, 18 (original), Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (see Doonan col. 6, lines 1-3: encrypted key is decrypted)

b) decrypting the messages with the user key. (see Doonan col. 6, lines 1-3: encrypted message is decrypted)

Regarding Claims 3, 11, 19 (currently amended), Doonan discloses the method, system and program product according to Claims 1, 9, 17, wherein: the encrypting data processing system further comprises a client system and a server system coupled for communication, said client system (see Doonan col. 3, lines 9-12: network connected client (sender) and server system) having a client memory device and said server system having an encryption chip and a server memory device:

a) storing the user key further comprises storing the user key in the client memory device; (see Doonan col. 9, lines 44-47: memory area used for data and workspace storage)

b) storing the associated key further comprises storing the associated key in the server memory device; (see Doonan col. 5, lines 4-5: key is stored at server system database)

c) Doonan discloses a check on the validation of a sender's credentials. (see Doonan col. 5, lines 16-20: sender credentials are verified) Doonan does not specifically disclose using a certificate authority (trusted third party) for key

validation and determination of key revocation. However, Sudia discloses preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device. (see Sudia col. 22, lines 51-63; col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to invalidate the association key when the status of the association key has been revoked as taught by Sudia. One of ordinary skill in the art would be motivated to employ Sudia in order to enable a trusted third party for a flexible and independent network key management system. (see Sudia col. 10, lines 23-25; col. 11, lines 15-23)

Regarding Claims 6, 14, 22 (currently amended), Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising: encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system. (see Doonan col. 2, lines 3-8: encryption key transferred to sender system)

Regarding Claims 7, 15, 23 (currently amended), Doonan discloses the method, system and program product according to Claims 6, 14, 22, further comprising: communicating an encrypted associated key to validate the association of the user with the encrypted messages. (see Doonan col. 5, lines 63-67:)

Regarding Claims 8, 16, 24 (original), Doonan discloses the method, system and program product according to Claims 7, 15, 23, further comprising: decrypting the associated key with the encryption chip key. (see Doonan col. 6, lines 1-3)

6. Claims 4, 12, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan-Sudia as applied to claims 1, 3 above, and further in view of Cook (US Patent No. 6,732,101).

Regarding Claims 4, 12, 20 (original), Doonan does not disclose a server system to receive, encryption and forward message. However, Cook discloses the method, system and program product according to Claims 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server system; (see Cook col. 2, lines 19-23: send message from client to server for encryption)
b) encrypting the messages using the encryption chip of the server system; (see Cook col. 2, lines 51-55: encrypt message)
c) sending the encrypted messages from the server system to the client system. (see Cook col. 2, lines 51-55: deliver encrypted message to recipient (client) system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to receive, encrypt and forward a message utilizing any encryption algorithm as taught by Cook. One of ordinary skill in the art

would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (see Cook col. 2, lines 33-38: *" ... Messages can be encrypted using any available encryption means at the sender and sent to a forwarding service. The forwarding service can forward the message to each recipient according to the recipient's decryption capability and preference. ... "*)

7. Claims 5, 13, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan-Sudia-Cook as applied to claims 1, 3, 4 above, and further in view of Marshall (US Patent No. 4,888,800).

Regarding Claims 5, 13, 21 (original), Doonan-Sudia-Cook does not disclose the ability to erase key information after processing of an encrypt message. However, Marshall discloses the method, system and program product according to Claims 4, 12, 20, further comprising: erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (see Marshall col. 2, lines 30-35: key information is erased from system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to erase all key related information after message processing maintaining only current information as taught by Marshall. One of ordinary skill in the art would be motivated to employ Marshall in order to enable a flexible and strengthened network key management system. (see Marshall col. 1, lines 50-58: *" ... system has the advantage ... only to maintain the keys required for whatever*

current communication sessions ... a pair of session keys ... every time a link or session is requested ... ")

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
Dec. 10, 2004

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100